Realtime publishers

The Shortcut Guide™ To

Subject Alternative Name Certificates

sponsored by

VeriSign®

Mike Danseglio

Copyright Statement

This sponsored eBook is valid until August 31, 2011.

Chapter 2: SAN Certificates In-Depth

Chapter 1 reviewed the basics of certificates. We established definitions for certificates and related technologies and processes. Although this information was a review for most readers, it is important to establish that common foundation before we press on to the more technical and complex topic of Subject Alternative Name (SAN) certificates.

This chapter will delve into the details of a SAN certificate. We'll examine the appropriate public key cryptography standards (PKCS), specifically the PKCS #10 and #7 certificate structures and meta data that apply to this technology. We'll compare data between SAN and non-SAN certificates. We will also compare SAN certificates to wildcard certificates to understand the distinction between two similar objects.

> **Note**
>
> Flip back to Chapter 1—particularly the Glossary—periodically as you read through this chapter, especially if you encounter a term that you're not familiar with (for example, CRL Distribution Point). Going back to Chapter 1 is also useful for recalling processes such as Secure Sockets Layer (SSL) cryptography.

What Is a SAN Certificate?

Why write a four-chapter guide about one very specific aspect of public key certificates? To put it in very simple terms, SAN certificates are amazingly powerful tools that you can use to solve important business problems inexpensively and efficiently. However, they must be used properly to realize the benefits and avoid potential drawbacks. We'll show you how to do both in this guide.

Overview

A SAN certificate is like most other certificates. It is requested with a PKCS #10 and supplied as a PKCS #7. But it has one important attribute that sets it apart from other, standard certificates. A SAN certificate has a field that specifies other domain names that can use the certificate.

Take, for example, a company that has a Web presence at Example.com. Most Internet users will open a browser and type http://www.example.com and land on the company's home Web page. But what happens when the company wants to switch to an SSL-restricted Web site? The company will probably redirect all requests from http://www.example.com to https://www.example.com and obtain an SSL-enabled certificate for that Web server. So far, so good.

But what happens when a user types https://example.com and presses Enter? Well, to SSL, the sites www.example.com and example.com are not the same. They have separate DNS namespaces. Or consider the impact a domain name purchase of Example.net or Example.org. The company will almost certainly want to use one Web site and simply provide the same content, including secure content, through the .net and .org domains. But the same problem as encountered earlier crops up because those are separate DNS namespaces. Thus, the same SSL certificate will not work on those Web sites.

The administrator could obtain a separate SSL certificate for each domain. But SSL certificates can be expensive to purchase individually. And unless a centralized system for automated certificate management and deployment is used, they are also more difficult to manage when there are a large number of them. In some cases, a more efficient deployment includes fewer, more flexible certificates.

SAN certificates fit this situation nicely. They allow Web servers in multiple DNS namespaces to share the same certificate. Let's take a look at how that happens.

Technical Details

Most certificates are actually pretty basic. As we saw in Chapter 1, they contain the basic information that allows them to establish their identity in a secure manner and then set up secure communication.

The purpose of a SAN certificate is the same as that of any other certificate. It provides a means for the server to establish its identity and then set up secure communication. It is really only different in one way: A SAN certificate contains a Subject Alternative Name field. This field specifies the DNS namespaces that can use the certificate. In basic certificates, the Subject field is the one that contains a fully qualified domain name (FQDN) and that FQDN is the only field that establishes the namespace where the certificate is valid. You can think of the Subject Alternative Name field as extending that namespace by including one or more additional namespaces.

Examining Certificate Details

To best understand the differences in these certificates, we can show actual certificates taken from live Web sites at the time of this writing. Note that by the time you read this chapter, the certificates may have changed. However, the information is still applicable.

Viewing Certificates with GUI vs. Text

You will probably notice that the certificates in this guide are displayed as screenshots from Microsoft Windows, specifically from the graphical user interface (GUI) of Windows Vista. There are important reasons to display them this way. The most important is that certificates are displayed in a very understandable and user-friendly manner in Windows. The various fields and values are parsed and presented in a tabbed dialog box. In addition, each certificate in the chain can be viewed and validated. Other operating systems (OSs) have similar presentation methods, parsing and displaying the data nicely.

If we chose to display the certificates in raw-text form, the usability would be quite different. For example, the following content is the actual data from the first certificate that we show in its native BASE64 format (a small amount has been deleted for space considerations):

-----BEGIN CERTIFICATE-----
MIIGvDCCBaSgAwIBAgIQB/3VFUtFQg6Qmkdyo+BLfTANBgkqhkiG9w0BAQUFADBp
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSgwJgYDVQQDEx9EaWdpQ2VydCBIaWdoIEFzc3VyYW5j
ZSBFViBDQS0xMB4XDTA4MDExNTAwMDAwMFoXDTEwMDMxNDIzNTk1OVowgf8xGzAZ
BgNVBA8MElYxLjAsIENsYXVzZSA1LihkKTETMBEGCysGAQQBgjc8AgEDEwJVUzEV
MBMGCysGAQQBgjc8AgECEwRVdGFoMRUwEwYDVQQFEww1Mjk5NTM3LTAxNDIxGzAZ
BgNVBAkTEjMzMyBTb3V0aCA1MjAgV2VzdDEOMAwGA1UEERMFODQwNDIxCzAJBgNV
BAYTAlVTMQ0wCwYDVQQIEwRVdGFoMQ8wDQYDVQQHEwZMaW5kb24xFTATBgNVBAoT
DERpZ2lDZXJ0IEluYzERMA8GA1UECxMIRGlnaUNlcnQxGTAXBgNVBAMTEHd3dy5k
aWdpY2VydC5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALXUnCJkdTU+
wc18EI7iSOad7mkbOyg5l18a8ThUFMUsZWPces5HZPrtlSjaQ+GI2QFDT9cBjqgA
msQzmouX4UYue4a0IuPjW7LigeqD53VEfcpb/Tm4xR7StDSNT0q3zXWb9g1rAO2K
N9sjGSckYS1IpADUxbqXcpGHZHeRQL+fAgMBAAGjggNLMIIDRzAfBgNVHSMEGDAW
gBRMWMsl8EFPUvQoyIFDm6aooOaS5TAdBgNVHQ4EFgQUaq4xHFUGsTaJb7Inzqb5
QRWrgrQwKQYDVR0RBCIwIIIQd3d3LmRpZ2ljZXJ0LmNvbYIMZGlnaWNlcnQuY29t
MDQGCCsGAQUFBwEBBCgwJjAkBggrBgEFBQcwAYYYaHR0cDovL29jc3AuZGlnaWNl
cnQuY29tMBEGCWCGSAGG+EIBAQQEAwIGwDAOBgNVHQ8BAf8EBAMCBaAwDAYDVR0T
AQH/BAIwADCBiwYDVR0fBIGDMIGAMD6gPKA6hjhodHRwOi8vY3JsMy5kaWdpY2Vy
dC5jb20vRGlnaUNlcnRIaWdoQXNzdXJhbmNlRVZDQS0xLmNybDA+oDygOoY4aHR0
cDovL2NybDQuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0SGlnaEFzc3VyYW5jZUVWQ0Et
-----END CERTIFICATE-----

If you think that's unusable, other formats are even worse. However, some programs, such as OpenSSL, have parsers that can read the encoded formats and present a more understandable description of a certificate. The following example is an older certificate from the University of Illinois at Urbana-Champaign:

```
Data:
    Version: 3 (0x2)
    Serial Number:
        fc:e7:90:e6:be:cd:e7:8b
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=US, ST=Illinois, L=Urbana, O=NCSA, OU=Security Research Division,
            CN=www.ncsa.uiuc.edu/emailAddress=webmaster@ncsa.uiuc.edu
    Validity
        Not Before: Mar  1 19:30:31 2006 GMT
        Not After : Mar  1 19:30:31 2007 GMT
    Subject: C=US, ST=Illinois, L=Urbana, O=NCSA, OU=Security Research Division,
             CN=www.ncsa.uiuc.edu/emailAddress=webmaster@ncsa.uiuc.edu
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (1024 bit)
            Modulus (1024 bit):
                00:b2:f3:ff:40:7e:29:78:0b:ec:2f:15:d9:b6:a7:
                bc:3a:b1:0b:19:a2:55:c9:43:52:74:ed:50:f2:48:
                2a:20:b9:70:a2:ea:c0:91:fc:0c:89:12:bf:44:ea:
                33:f7:e7:41:6c:80:5a:0c:9f:87:74:aa:19:01:6f:
                a2:70:73:32:6d:25:13:e9:85:92:2f:5d:38:b4:ae:
                b3:b3:66:97:b4:c9:31:75:ec:d5:9c:73:95:d7:9f:
                d3:3c:31:b4:76:8d:2f:7b:a6:32:76:03:27:25:bc:
                e8:06:37:f9:d8:21:d1:29:05:f1:8a:27:47:0b:42:
                be:74:ac:11:00:bb:e1:92:71
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Subject Key Identifier:
            0F:54:DA:9E:36:1D:1E:B8:C4:82:B7:B8:AF:53:AA:CB:81:62:4A:2B
        X509v3 Authority Key Identifier:
            keyid:0F:54:DA:9E:36:1D:1E:B8:C4:82:B7:B8:AF:53:AA:CB:81:62:4A:2B
```

DirName:/C=US/ST=Illinois/L=Urbana/O=NCSA/OU=Security Research Division/
CN=www.ncsa.uiuc.edu/emailAddress=webmaster@ncsa.uiuc.edu
serial:FC:E7:90:E6:BE:CD:E7:8B

X509v3 Basic Constraints:
CA:TRUE
Signature Algorithm: sha1WithRSAEncryption
07:ea:e7:68:38:a0:c5:45:b7:3a:79:da:93:19:7a:fc:68:bf:
d1:f2:24:da:6e:58:73:8f:ef:2e:d6:1e:6b:98:ce:28:03:cb:
9b:ce:a8:98:0f:92:2d:f0:de:19:1d:a6:b2:0a:28:86:f9:ed:
43:f0:7c:46:71:ad:6e:16:c2:49:56:96:57:18:57:6f:f4:d3:
2b:59:f6:d7:f9:1a:b7:86:84:cf:80:18:a3:99:ce:ff:9f:0d:
00:6d:cc:ba:f8:4f:84:ce:8e:94:0e:1e:d7:1e:89:1d:49:78:
d3:55:1c:bf:98:e7:77:17:6c:fe:aa:2a:1d:13:62:7f:31:55:
01:f7

I recommend that you stick to GUI-based certificate management as a rule, using text-based command-line tools only when necessary to closely examine or manipulate granular data.

Figure 2.1 shows a certificate with only one valid namespace, taken from a well-known US financial site.

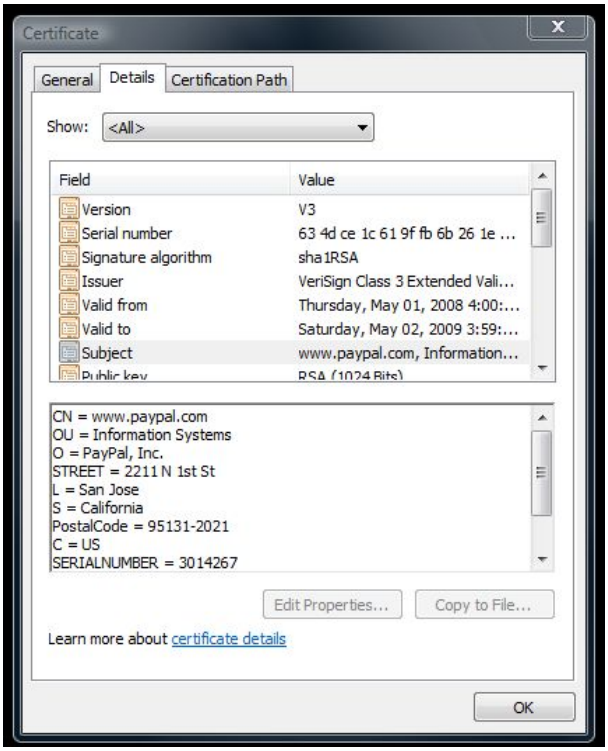

Figure 2.1: A common-name certificate without the Subject Alternative Name field.

This certificate is valid and provides the required security and authentication. However, it protects only the namespace defined in the Common Name (CN) portion of the Subject field. Figure 2.2 shows a SAN certificate.

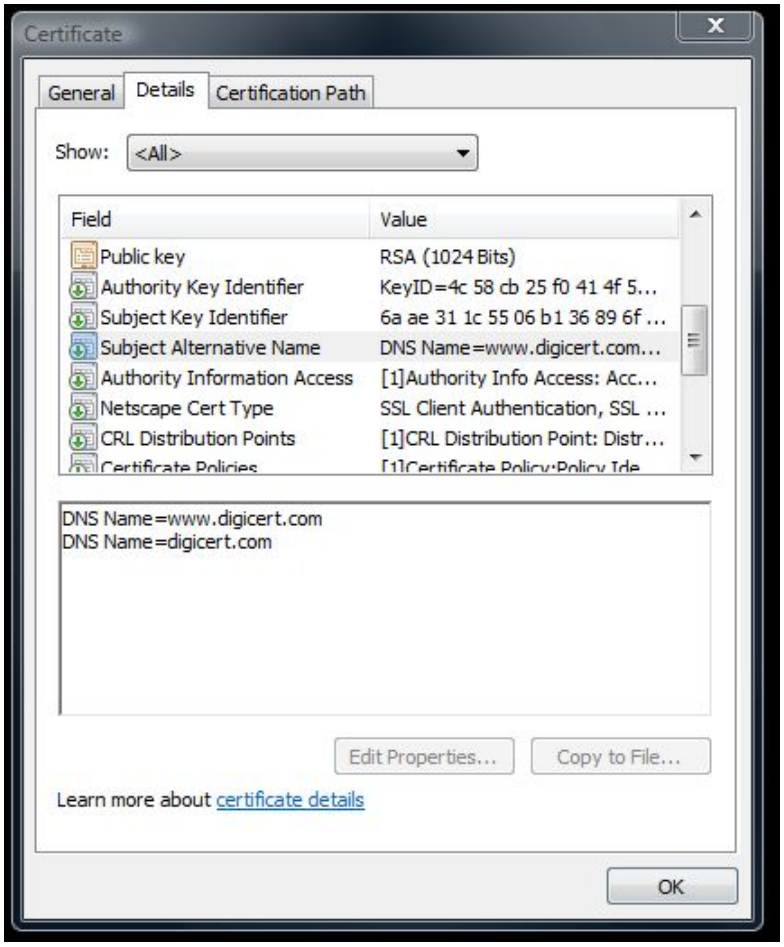

Figure 2.2: A certificate that includes a Subject Alternative Name field.

The SAN field is simply a list of extra DNS namespaces. When the client receives the certificate from the server, it checks both the Subject and SAN fields to verify that the certificate is in use on the correct server. If any matches exist—that is, if the server matches any of the DNS paths listed—the certificate is valid.

Uses For SAN Certificates

You now have a pretty good idea of what SAN certificates do and how they do it. But how is it directly applicable to your existing PKI or server infrastructure?

The most interesting uses of SAN certificates today are in the areas of email and instant messaging (IM). With the release of new software that utilizes the full potential of SAN certificates, administrators can use them much more easily and optimize the use of every certificate even further. The use of SAN certificates in SSL configurations has been only briefly covered, so we'll discuss that more thoroughly as well.

> **Note**
>
> This section will describe the scenarios that make good use of SAN certificates. However, we will not be listing step-by-step instructions about how to implement SAN certificates. Chapter 3 will provide more specific details on exactly how to operate with these certificates.

Email

Using PKI certificates that chain to a trusted root is very important in any email infrastructure. To prevent attackers from spoofing a valid system, the email clients must know that the server is authentic and trustworthy before they transmit or receive sensitive data. Similarly, email servers must know that their peers (other email servers) are authentic to avoid including rogue servers in their email distribution channel. Failure of these security measures could easily allow an attacker to send false email or intercept others' email, often without detection.

Many large organizations segment their email and authentication into manageable portions. This division is often done along geographic boundaries, but the segmentation can be along any lines that make business sense, such as departmental.

With our favorite example organization, Example.com, let's assume that there are tens of thousands of users. Putting all users in one database could easily choke most systems, degrading performance and making administration difficult. For that reason, Example.com divides its user base into geographic groupings. A user from France, for example, will login to the France.Example.com domain and has an email address of *username*@France.Example.com. A user from the US would be *username*@US.Example.com, and so forth. This setup makes sense from an administrative viewpoint.

From the PKI viewpoint, this division is a nightmare. Each subdomain is a different namespace. Thus, each requires a different certificate. Worse yet, depending on the certification authority (CA), different validation and application may be required for each certificate. For example, some vendors have different requirements depending on whether the certificate applies to a .com, .org, or .net domain name.

Using a SAN certificate in this situation is perfect. A single SAN certificate can, for example, contain a field that allows servers in the following domains to provide authentication:

```
Example.com
*.Example.com
*.US.Example.com
*.Japan.Example.com
*.France.Example.com
```

Thus, all the email servers for Example.com can share one SAN certificate.

Proper Use of SAN Certificates

Prior to the release of Microsoft Exchange 2007, SAN certificates were not properly processed by most email servers. Although the SAN field has been a part of the PKI standards for many years, few software vendors originally took advantage of this feature. As a result, few SAN certificates were used to their full potential. Other alternatives were used, including wildcard certificates (discussed later).

Starting with Microsoft Exchange 2007 and continuing to other products, proper use of SAN certificates has begun to drive the popularity of this deployment technique. In fact, other messaging technologies have begun to take advantage of the flexibility and power of SAN certificates. Today, many software packages use it, and in fact, some (Microsoft Office Live Communications Server in particular) require this type of certificate for operation.

Instant Messaging

Similar to the email paradigm explored in the previous section, IM requires certificates for server-to-client and server-to-server authentication and secure communication establishment. However, this paradigm is relatively new in corporate computing. Let's take a bit of a closer look at it.

Industry and social trends are moving towards smaller, frequent, and more informal communications. Consider the type of text messaging that virtually all modern cell phones support. The messages are short—less than 160 characters per message with no attachments. This type of communication has branched into several technologies, one of the more popular being IM.

Because IM gained most of its exposure with informal, leisure-oriented communication, many business decision makers (BDM) have overlooked IM as a component of business communications. But over the past several years, IM has been gaining popularity and more widespread use in business environments. As a result, business-oriented IM solutions have begun to surface. These are led by Microsoft's Office Communications Server 2007 (OCS) product.

OCS offers a great deal of communications technologies including integration with email and Voice over IP (VoIP) telephony services. One of the more interesting offerings is an IM server and client. Because OCS allows an enterprise to host its own IM infrastructure, administrators can apply security and usage policies and manage the infrastructure in compliance of company policy. Users no longer have to resort to using public (and likely less secure) technologies such as Skype or Yahoo Instant Messenger to communicate.

There are often many very similar OCS servers configured in groups to handle the heavy load sometimes experienced during busy times or events. For example, Monday morning is a very busy time for any IM infrastructure. People are beginning their work week, catching up on weekend experiences, planning their week, and so on. Often, these communications are most appropriate for IM-style communication. Communications servers can also reach peak load during important events, such as a company laying off employees or announcing a merger. As a result of this type of load, some companies can have hundreds of IM servers running OCS spread out over the infrastructure to disperse load and ensure that they are near the clients for optimal bandwidth and performance. These servers must be configured in a near-identical faction.

As you may have surmised, OCS uses public key certificates. One important function of OCS is its use of SAN certificates to authenticate and establish secure communications channels. If each has a unique certificate, it greatly increases the workload of renewing and replacing certificates and decreases the security of the infrastructure by exposing more systems if a key is compromised. That is, if a certificate is compromised, an attacker has broken the "chain of trust" and all systems that trust that certificate are also vulnerable as they now trust a compromised certificate.

> **Note**
> Whenever a private key is exposed or broken, regardless of the PKI design, the infrastructure is at risk to some degree. Different designs can help to minimize this exposure, but they may be suboptimal in other areas. This concern is one you most likely considered when deciding on your PKI design.

OCS does not support wildcard certificates for the common name in a certificate. A SAN certificate must be used for this solution.

Secure Sockets Layer

Probably the most common use of certificates in a PKI environment is for serving up SSL communications. You already know the basics of SSL from Chapter 1 and from connecting to secure Web sites. Virtually all secure Web sites (and many services) use SSL in one capacity or another.

What you might not have encountered yet is how difficult certificate management can be in an SSL environment. If each server uses a separate certificate, the user experience must be carefully tested (to ensure trust works properly), and the administration is a nightmare without an automated certificate management platform (frequently called *managed PKI*) in place. A wildcard certificate can be useful but has some limitations (described later), especially when you have multiple DNS namespaces. A SAN certificate can be useful in this configuration with its ability to provide SSL for multiple namespaces.

Now that we've established the business and technical uses for a SAN certificate and the details of what distinguishes a SAN certificate, let's take a look at how to actually obtain one.

Requesting and Receiving a SAN Certificate

The process of requesting and receiving a SAN certificate can be either very simple or very complex. It almost entirely depends on your PKI. There are a few key elements of this process that will apply regardless of your specific topology. First, you need to identify your resources to determine whether you really need a SAN certificate. Then, you'll need to determine what DNS names need to be included in the Subject Alternative Name field and what uses your certificate will have. Once you've acquired that data, you can request the certificate and install it once issued. Let's briefly look at each part of this process.

Identifying Resources and Uses

We've seen the main purposes for SAN certificates. They're very useful in environments that use Microsoft OCS or Exchange 2007 products where multiple DNS namespaces are part of the corporate infrastructure. They're also useful in some SSL-enabled environments with multiple DNS namespaces.

If you have this software in your environment, you most likely need a SAN certificate (or a large number of standard certificates, which is both expensive and inefficient). Although having a Subject Alternative Name field in a certificate that is not used for one of these purposes does not hurt anything, it may not be the best security practice. Most security practitioners tend to minimize and simplify configurations, keeping to the "less is more" axiom. Because the SAN field in the certificate may be extraneous data, you should weigh whether that field would impact your security posture.

You must identify the specific applications and servers that will use the new certificate. This identification is absolutely critical to ensuring that you obtain the appropriate certificate. If you're using an outsourced PKI that charges per certificate, you already know that requesting an improper certificate is a costly mistake. It can be even more costly if the mistake is discovered after the certificate is deployed.

Consider gathering the following information:

- Applications that will use the SAN certificate, especially OCS and Exchange—The list of applications will ensure that you specify both the proper domain names and the proper Key Usage and Extended Key Usage fields in the certificate.
- Servers that will run the software that uses the SAN certificate, and their DNS names—This information is critical to ensuring that your Subject Alternative Name field is complete and correct.
- Other PKI-enabled servers that may benefit from using this certificate, and their DNS names—You may find that you want to use a single SAN-enabled certificate more broadly than first thought as you continue to gather information.

Note

You might already have this information. Most well-run networks already have a complete network map and inventory of systems and their functions. If you have that data, congratulations! This task will be quick and easy. However, if you don't have this data, you should consider gathering it and keeping it up-to-date for a variety of reasons, not the least of which is for PKI planning. There are dozens of software tools and process guidance packages that will help you accomplish this task, ranging from enterprise-class fully automated software to simple, free utilities that can gather the information for you in a matter of moments.

Once you have this data, you should have enough information to obtain a SAN certificate. Of course, the certificate request will differ depending on whether you manage your own PKI or use a managed or external system. So let's take a look at these in more detail.

Obtaining the Certificate

How do you obtain a SAN certificate? The simple answer is: the same way you obtain any other certificate. You already have some PKI integration with your network. Obtaining a SAN certificate is done the same way as acquiring a Web Server or Recovery Agent certificate.

In very general terms, there are two approaches to PKI. Each has its own approach to requesting and retrieving a certificate. You either manage your own PKI or you use an outsourced commercial PKI. The two are very different and require individual explanation.

Outsourced PKI

Not very long ago, there were only a small handful of PKI vendors that offered truly useful certificates (certificates that chained to an already trusted public root CA) at a reasonable price. But times have changed. There are hundreds of PKI vendors in the world today. Many of them offer amazing products and very reasonable prices. Virtually all of them chain to a trusted root. And most of them offer a variety of levels of assurance, such as Extended Validation (see Chapter 1) and chaining to different root certificates depending on the level of trust required.

One important selling point for PKI vendors has been the ease of use of their products. Because, let's face it, PKI deployment and operation is difficult. Having a commercial offering that is just as difficult as an internal deployment makes no sense. Thus, PKI vendors have gone to great lengths to make their products simple to use. Many have simplified the certificate request process to a basic Web-based form or a browser plug-in, reducing the entire process to less than a minute's work. Often a Web-based certificate enrollment process is accompanied by a phone call to Customer Service or interactive online assistance. Honestly, they couldn't make it much easier to get a certificate.

The key element in successfully obtaining a SAN certificate from an outsourced PKI vendor is communicating the information that you gathered in the previous step. The vendor cannot read your mind and determine that you need a SAN certificate with *x* domains or *y* key usage fields. Consider creating a complete document of the information that you gathered and providing it to the vendor along with the certificate request to avoid any confusion. Although it might seem like overkill, it is certainly better to err on the side of completeness and redundancy than risk a useless $5000 certificate (as an example—not all certificates cost $5000).

The certificate is normally issued through a safe means. Some vendors send a CD or USB drive to the address provided during enrollment as an additional security verification. Others use an SSL Web site or even secure email to provide the certificate. Regardless of the method of issuance, you should immediately examine the certificate to verify that the required data, especially the Subject Alternative Name field, is correct.

Internally Managed PKI

Managing your own PKI used to be a daunting task. You needed to hire or become a PKI guru. You needed to read at least one book on the topic. You had to become an expert on the OS that supported the PKI and the client systems and applications that used certificates. All that before you even decided on whether to use an internal or external PKI solution and have deployed the PKI!

Times have changed. PKI is much more approachable and easy to deploy and operate. Some OSs, such as Windows Server 2003 and Windows Server 2008, have a CA software package built right in. With a basic knowledge of PKI and the client requirements, you can have a self-signed PKI up and running in less than an hour, and a CA that chains to an external trusted root in only a little more time than that. And most of these software packages make certificate requests extremely simple.

For example, let's take a look at Windows Server 2008. Assuming you've got a CA installed and configured (a wizard-driven task that takes just a few moments), how do you request a SAN certificate? By default, Windows Server 2008 installs its own Web-based certificate management Web site on the CA at http://*servername*/certsrv. The default Web page isn't glamorous or colorful, but it is both highly functional and customizable (see Figure 2.3).

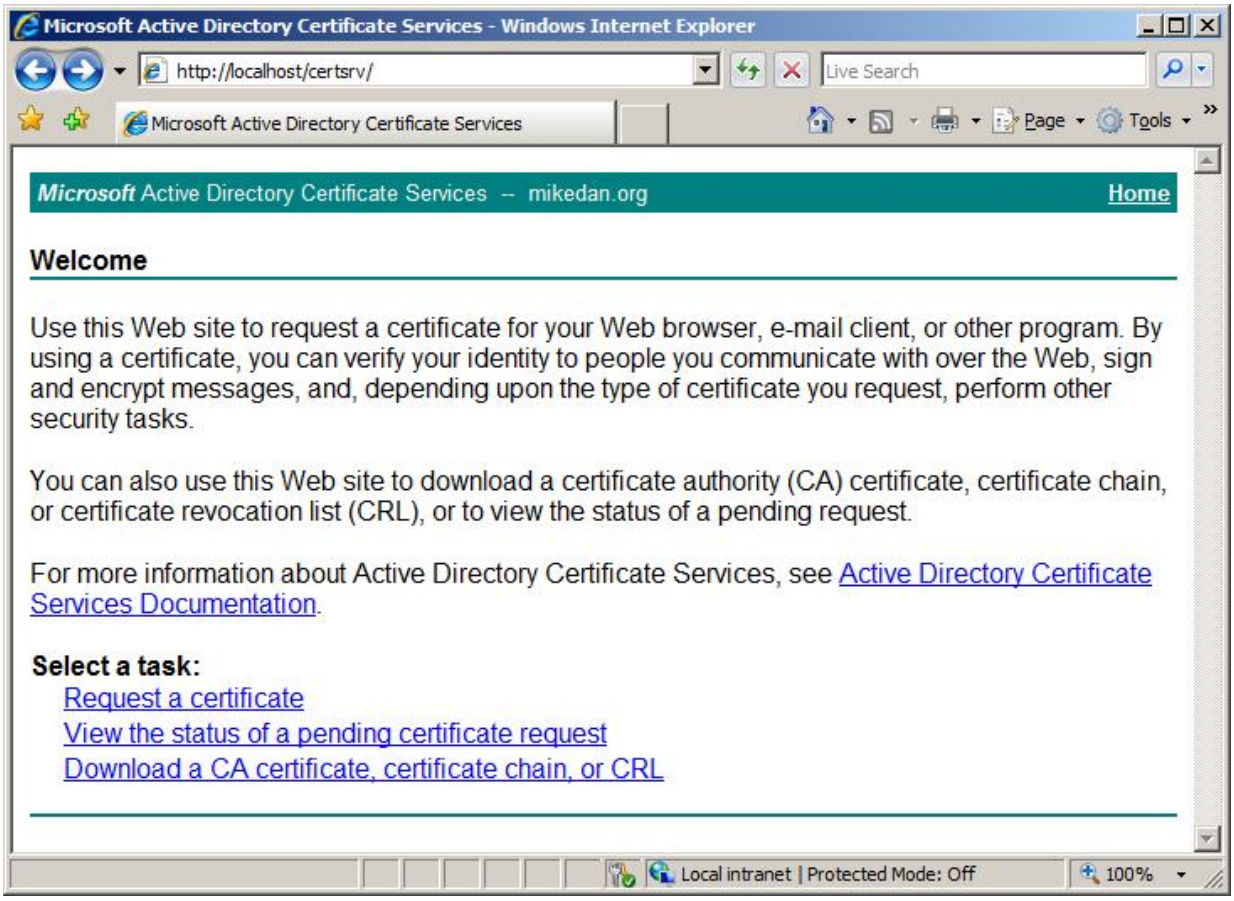

Figure 2.3: The default Windows Server 2008 CA home page.

You can see in Figure 2.3 that the key elements of certificate enrollment are available: request a certificate and view the status of a certificate (or retrieve an issued certificate). Clicking *Request a certificate* results in a fairly complete form that you can use to either fill out and specify the request or submit a binary-encoded request that comes from your software package (Figure 2.4).

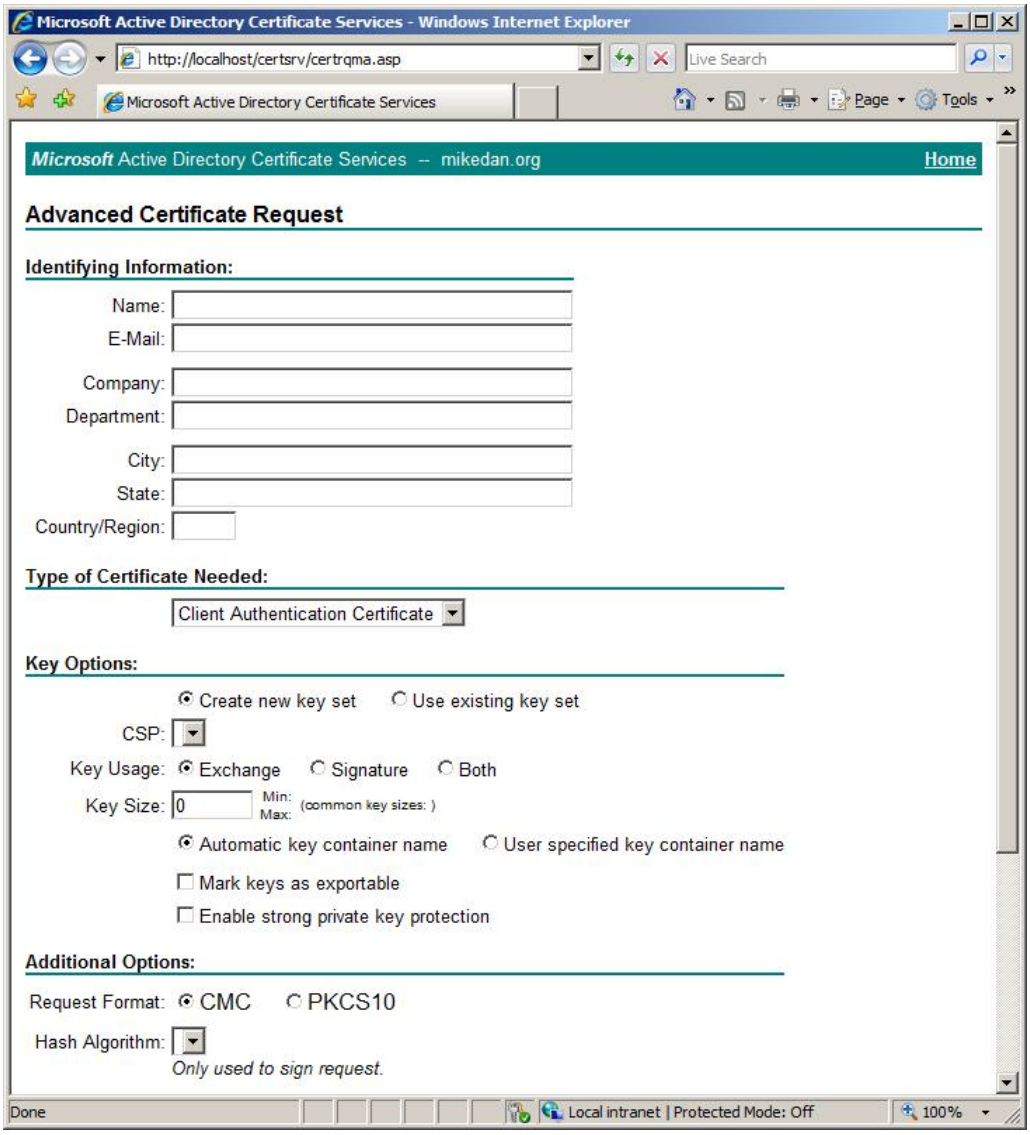

Figure 2.4: The Certificate request page. Not shown at the bottom (for space concerns) is a text field where you can simply paste in a binary-encoded certificate request from your favorite application.

For most certificate requests, you will create a CMC or PKCS #10 request with your favorite application and then paste it in to this form. Doing so ensures that the desired fields, especially the Subject Alternative Name field, are complete and correct. In Windows Server 2008, the command-line tools Certreq.exe and Certutil.exe can be used to create the request and submit it directly to the CA.

More Information

For complete documentation of the PKCS #10 format, see http://www.rsa.com/rsalabs/node.asp?id=2132 and http://www.ietf.org/rfc/rfc2986.txt. For a very readable example, see http://msdn.microsoft.com/en-us/library/aa379078(VS.85).aspx. For a lengthy article on using Certreq.exe and Certutil.exe to create and submit a SAN certificate request, see http://support.microsoft.com/kb/931351.

Wildcard Certificates

By now, you've seen the strengths and weaknesses of SAN certificates. You might already be familiar with another certificate type that fills a similar role—wildcard certificates are simply certificates that allow you to secure multiple first-level child domains based on one root domain. For example, if you have a *.Example.com wildcard certificate, you can secure mail.Example.com and www.Example.com with that same wildcard certificate.

However, you cannot secure second-level child domains or disjointed domains (for example, Example.com and Example.org) with wildcard certificates. That is where the flexibility of SAN certificates comes in. Although wildcard certificates have uses, they are not as flexible and powerful as SAN certificates. In addition, many small browsers (such as those found on phones or ultraportable devices) and other portable applications do not understand how to process wildcard certificates properly. These same applications often work well with SAN certificates. If you intend to support portable clients on your network, determine whether wildcard certificates work and ensure that your PKI supports whatever certificates are required. However, you should note that wildcard certificates can be considered somewhat of a security risk due to their unrestricted nature. Even if they will meet the technical needs of your deployment, they may present more security exposure than acceptable.

Summary

This chapter provides a deeper look into SAN certificates. We examined exactly what distinguishes this type of certificate—the Subject Alternative Name field. We also saw what that field looks like in real certificates.

This chapter also showed the Windows Server 2008 CA in more depth, including how to obtain a SAN certificate. Although you might not be using Windows Server 2008 in your PKI, the information in this chapter applies to most PKI software. If you're using an outsourced PKI, the tasks are almost always easier because of the customization and extensive customer service that they provide.

Throughout the chapter, we also looked at wildcard certificates. You shouldn't come away from this chapter believing that SAN certificates are superior to wildcard certificates. Each has their own role in an organization. You may, depending on your network and PKI architecture, decide to use one or the other, or both. The only "wrong" way to use these certificates is if the way they're being used prevents applications from working correctly.

We focused on the technical side of certification in this chapter. In the next chapter, we will explore the business side of SAN certificates. We'll examine how they make sense, where they make sense, and what business functions they support. Because all certificates have a real cost to an organization, we'll look at the return on investment side of things to help you make the most cost-effective choices possible.